CUBE(Cisco Unified Border Element) Enterprise 장치 강화에 대한 Cisco 설명서

목차

소개

이 문서는 CUBE(Cisco Unified Border Element) Enterprise를 실행하는 SBC(Session Border Controller) 역할을 하는 Cisco IOS 및 IOS-XE 디바이스를 보호하고 강화하는 데 도움이 될 것입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

- IOS-XE 17.10.1a를 실행하는 CUBE Enterprise

참고:

이전 버전의 IOS-XE에서는 이 문서에 설명된 기능 중 일부를 사용하지 못할 수 있습니다. 명령이나 기능이 도입되거나 수정되었을 때 문서화하는 데 주의해야 하는 경우

이 문서는 CUBE Media Proxy, CUBE Service Provider, MGCP 또는 SCCP 게이트웨이, Cisco SRST 또는 ESRST 게이트웨이, H323 게이트웨이 또는 기타 아날로그/TDM 음성 게이트웨이에 적용할 수 없습니다.

배경 정보

이 문서는 Cisco Guide to Hardened Cisco IOS Devices에서 찾아볼 수 있는 것에 대한 추가 자료입니다. 따라서 해당 문서의 중복 항목은 이 문서에서 중복되지 않습니다.

CC(Common Criteria) 및 FIPS(Federal Information Standard)

CSR1000v 또는 CAT8000v에서 IOS-XE 16.9+를 사용하는 Cisco Virtual CUBE는 cc-mode 명령을 사용하여 TLS(Transport Layer Security) 및 와 같은 다양한 암호화 모듈에서 CC(Common Criteria) 및 FIPS(Federal Information Standards) 인증 시행을 활성화할 수 있습니다. 하드웨어 라우터에서 실행되는 CUBE에 대해 equivalent 명령은 없지만 이후 섹션에서는 유사한 강화 기능을 수동으로 활성화하는 방법을 제공합니다.

출처: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_cc_fips_compliance.html

TLS(Transport Layer Security) 및 PKI(Public Key Infrastructure)

이 섹션에서는 SIP(Secure Session Initial Protocol) 및 SRTP(Secure Real Time Protocol) 작업과

함께 이러한 프로토콜에서 제공하는 보안을 강화할 수 있는 TLS 및 PKI에 대한 항목을 다룹니다.

TCP TLS 및 SRTP 사용

기본적으로 CUBE는 TCP, UDP 또는 SIP TCP-TLS를 통한 인바운드 SIP 연결을 허용합니다. 아무것도 구성되지 않으면 TCP-TLS 연결이 실패하지만, CUBE에서 TCP 및 UDP를 수락하고 처리합니다. 아웃바운드 연결의 경우 TCP 또는 TCP-TLS 명령이 없으면 SIP는 기본적으로 UDP 연결을 사용합니다. 마찬가지로 CUBE는 비보안 RTP(Real Time Protocol) 세션을 협상합니다. 두 프로토콜 모두 공격자가 암호화되지 않은 SIP 세션 신호 또는 미디어 스트림에서 데이터를 삭제할 수 있는 충분한 기회를 제공합니다. 가능한 경우 SIP TLS를 사용하여 SIP 신호 처리를 보호하고 SRTP를 사용하여 미디어 스트림을 보호하는 것이 좋습니다.

SIP TLS 컨피그레이션 및 SRTP 컨피그레이션 설명서를 참조하십시오.

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_sip_tls_support_cube.html
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_cc_fips_compliance.html?bookSearch=true#id_118373

보안은 가장 약한 링크만큼 강력하며 CUBE를 통해 모든 호출 레그에 대해 SIP-TLS 및 SRTP를 활성화해야 합니다.

나머지 섹션은 추가 보안 기능을 제공하기 위해 이러한 기본 컨피그레이션에 추가됩니다.

비보안 SIP 포트 비활성화

CUBE가 기본적으로 CUBE에 대한 인바운드 TCP 및 UDP를 수락한다는 자세한 내용은 이전 섹션을 참조하십시오. 모든 통화 레그에 대해 SIP TLS가 사용되면 안전하지 않은 UDP 및 TCP SIP 수신 대기 포트 5060을 비활성화하는 것이 바람직할 수 있습니다.

비활성화되면 show sip-ua status, show sip connections udp brief 또는 show sip connections tcp brief를 사용하여 CUBE가 5060에서 인바운드 TCP 또는 UDP SIP 연결을 더 이상 수신하지 않음을 확인할 수 있습니다.

```
<#root>

Router#

show sip-ua status


SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED

Router#

show sip connections udp brief | i 5060


0 [0.0.0.0]:5060: 0
```

```
Router#
show sip connections tcp brief | i 5060

0 [0.0.0.0]:5060: 0!



!
sip-ua
 no transport udp
 no transport tcp
!
```

<#root>

```
Router#
show sip-ua status

SIP User Agent Status
SIP User Agent for UDP :
DISABLED

SIP User Agent for TCP :
DISABLED

SIP User Agent for TLS over TCP : ENABLED
Router#
show sip connections tcp brief | i 5060

Router#
show sip connections udp brief | i 5060
```

CUBE는 IOS-XE VRF와 함께 작동하여 추가 네트워크 세그멘테이션을 제공하도록 구성할 수도 있습니다.

VRF를 구성하고 VRF 지원 인터페이스를 다이얼 피어/테넌트에 바인딩함으로써 CUBE는 해당 IP, 포트, VRF 조합에 대한 인바운드 연결만 수신합니다.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-cube-multi-vrf.html

TLS 1.2 적용

이 문서를 작성할 때 TLS 1.2는 CUBE에서 지원하는 가장 높은 버전의 TLS입니다. IOS-XE 16.9에서 TLS 1.0을 사용할 수 없지만 TLS 1.1을 협상할 수 있습니다. TLS 핸드셰이크 중에 옵션을 추가로 제한하려면 관리자가 CUBE Enterprise에 대해 사용 가능한 유일한 버전을 TLS 1.2로 강제 지정할 수 있습니다

```
!
sip-ua
 transport tcp tls v1.2
!
```

TLS 암호 적용

약한 TLS 암호가 세션에서 협상되지 않도록 설정하는 것이 바람직할 수 있습니다. IOS-XE 17.3.1부터 관리자는 TLS 프로파일을 구성할 수 있으며, 이를 통해 관리자는 TLS 세션 중에 어떤 TLS 암호가 제공될지 정확히 정의할 수 있습니다. 이전 버전의 IOS-XE에서는 crypto signaling sip-ua 명령에서 strict-cipher 또는 ecdsa-cipher postfix를 사용하여 제어되었습니다.

선택하는 암호는 CUBE와 SIP TLS를 협상하는 피어 디바이스와 호환되어야 합니다. 모든 장치 간의 최상의 암호를 확인하려면 해당 공급업체 설명서를 모두 참조하십시오.

IOS-XE 17.3.1+

```
<#root>

Router(config)#

voice class tls-cipher 1


Router(config-class)#

cipher ?


<1-10> Set the preference order for the TLS cipher-suite (1 = Highest)
Router(config-class)#

cipher 1 ?


   DHE_RSA_AES128_GCM_SHA256       supported in TLS 1.2 & above
   DHE_RSA_AES256_GCM_SHA384       supported in TLS 1.2 & above
   DHE_RSA_WITH_AES_128_CBC_SHA    supported in TLS 1.0 & above
   DHE_RSA_WITH_AES_256_CBC_SHA    supported in TLS 1.0 & above
   ECDHE_ECDSA_AES128_GCM_SHA256   supported in TLS 1.2 & above
   ECDHE_ECDSA_AES256_GCM_SHA384   supported in TLS 1.2 & above
   ECDHE_RSA_AES128_GCM_SHA256     supported in TLS 1.2 & above
   ECDHE_RSA_AES256_GCM_SHA384     supported in TLS 1.2 & above
   RSA_WITH_AES_128_CBC_SHA        supported in TLS 1.0 & above
   RSA_WITH_AES_256_CBC_SHA        supported in TLS 1.0 & above
```

```
!
voice class tls-cipher 1
 cipher 1 ECDHE_RSA_AES128_GCM_SHA256
 cipher 2 ECDHE_RSA_AES256_GCM_SHA384
!
voice class tls-profile 1
 trustpoint TEST
 cipher 1
!
sip-ua
 crypto signaling default tls-profile 1
!
```

기타 모든 버전

<#root>

```
! STRICT CIPHERS
sip-ua
 crypto signaling default trustpoint TEST
```

strict-cipher

```
 ! Only Enables:
 ! TLS_RSA_WITH_AES_128_CBC_SHA
 ! TLS_DHE_RSA_WITH_AES_128_CBC_SHA1
 ! TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 ! TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384



!
! ECDSA Ciphers
sip-ua
 crypto signaling default trustpoint TEST
```

ecdsa-cipher

```
 ! Only Enables:
 ! TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 ! TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
!
```

대형 암호화 키 활용

Cisco Next Generation Cryptography 표준에서는 2048년에 TLS 1.2 애플리케이션과 함께 사용할 것을 권장합니다. 아래 명령을 사용하여 TLS 세션에 사용할 RSA 키를 만들 수 있습니다.

label 명령을 사용하면 관리자가 신뢰 지점에서 이러한 키를 쉽게 지정할 수 있으며 내보낼 수 있는 명령을 사용하면 필요한 경우 다음과 같은 명령을 사용하여 프라이빗/퍼블릭 키 쌍을 내보낼 수 있습니다

암호화 키 내보내기 rsa CUBE-ENT pem 터미널 aes 암호!123

<#root>

```
!
crypto key generate rsa general-keys modulus 2048 label CUBE-ENT exportable
!
```

Router#

show crypto key mypubkey rsa CUBE-ENT

```
% Key pair was generated at: 11:38:03 EST Mar 10 2023
Key name: CUBE-ENT
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is exportable. Redundancy enabled.
 Key Data:
  [..truncated..]
```

CA(Certificate Authority) 서명 인증서 활용

관리자는 CUBE Enterprise용 신뢰 지점 및 ID(ID) 인증서를 생성할 때 자체 서명 인증서 대신 CA 서명 인증서를 사용해야 합니다.

CA 인증서는 일반적으로 CRL(Certificate Revocation List) 또는 OCSP(Online Certificate Status Protocol) URL과 같은 추가 보안 메커니즘을 제공하며, 이는 인증서가 폐기되지 않았음을 확인하기 위해 디바이스에서 사용할 수 있습니다. 신뢰할 수 있는 공용 CA 체인을 사용하면 잘 알려진 루트 CA에 대한 트러스트가 포함되어 있거나 엔터프라이즈 도메인에 대한 루트 CA 트러스트가 이미 있는 피어 디바이스에서 트러스트 관계 컨피그레이션을 쉽게 수행할 수 있습니다.

또한 CA 인증서는 Basic Constraints(기본 제약 조건)에서 True(참)의 CA 플래그를 포함해야 하며 CUBE의 ID 인증서에는 Client Auth(클라이언트 인증)의 Extended Key Usage(확장 키 사용) 매개변수가 포함되어야 합니다.

다음은 CUBE용 샘플 루트 CA 인증서 및 ID 인증서입니다.

openssl x509 -in some-cert.cer -text -noout

<#root>

```
### Root CA Cert


Certificate:
[..truncated..]
 X509v3 extensions:
```

X509v3 Basic Constraints

:

critical

CA:TRUE

, pathlen:0
[..truncated..]
   X509v3

Extended Key Usage

:
     TLS Web Server Authentication, TLS Web

Client Authentication

[..truncated..]

ID Cert

Certificate:
 Data:
[..truncated..]
  Signature Algorithm:

sha256WithRSAEncryption

[..truncated..]
  Subject Public Key Info:
   Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

[..truncated..]
  X509v3 extensions:
   X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
[..truncated..]
   X509v3

Extended Key Usage

:
    TLS Web Server Authentication,

TLS Web Client Authentication

[..truncated..]

강력한 해시 활용

CUBE의 ID 인증서에 대한 신뢰 지점을 구성할 때 SHA256, SHA384 또는 SHA512와 같은 강력한 해싱 알고리즘을 선택해야 합니다.

```
Router(config)#
 crypto pki trustpoint CUBE-ENT

Router(ca-trustpoint)#
hash ?

 md5 use md5 hash algorithm
 sha1 use sha1 hash algorithm
 sha256 use sha256 hash algorithm

 sha384 use sha384 hash algorithm

 sha512 use sha512 hash algorithm
```

CRL(Certificate Revocation List) 또는 OCSP(Online Certificate Status Protocol) 확인 사용

기본적으로 IOS-XE Trustpionts는 crypto pki auth 명령 동안 인증서 내에 나열된 CRL을 확인하려고 시도하며, 나중에 TLS 핸드셰이크 동안 IOS-XE는 수신된 인증서를 기반으로 다른 CRL 가져오기를 수행하여 인증서가 여전히 유효한지 확인합니다. CRL의 방법은 HTTP 또는 LDAP일 수 있으며 성공하려면 CRL에 대한 연결이 있어야 합니다. 즉, 서버에서 IOS-XE 라우터로 DNS 확인, TCP 소켓 및 파일 다운로드를 사용할 수 있어야 합니다. 그렇지 않으면 CRL 검사가 실패합니다. 마찬가지로 IOS-XE 신뢰 지점은 HTTP를 통해 OCSP 응답자에 쿼리를 수행하여 유사한 검사를 수행하고 검사하도록 인증서 내의 AIA(AuthorityInfoAccess) 헤더에서 OCSP 값을 사용하도록 구성할 수 있습니다. 관리자는 인증서에 고정 URL을 제공하여 인증서 내에서 OCSP 또는 CDP(CRL Distribution Point)를 재정의할 수 있습니다. 또한 관리자는 CRL 또는 OCSP가 둘 다 있다고 가정하여 점검되는 순서를 구성할 수도 있습니다.

많은 경우 프로세스를 간소화하기 위해 revocation-check none으로 폐기 검사를 비활성화하지만, 이를 통해 관리자는 보안을 약화시키고 지정된 인증서가 여전히 유효한지 상태를 확인하기 위해 IOS-XE의 메커니즘을 제거합니다. 가능한 경우 관리자는 OCSP 또는 CRL을 활용하여 수신된 인증서의 상태 기반 검사를 수행해야 합니다. CRL 또는 OCSP에 대한 자세한 내용은 다음 문서를 참조하십시오.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book/sec-cfg-auth-rev-cert.html

CRL 검사

<#root>

```
! Sample A: CRL from the certificate

crypto pki trustpiont ROOT-CA
```

```
 revocation-check crl
!

! Sample B: CRL Override OCSP in certificate


crypto pki certificate map CRL-OVERRIDE 1
 issuer-name eq root-ca.cisco.com
 subject-name eq root-ca.cisco.com
 alt-subject-name co cisco.com
!
crypto pki trustpoint ROOT-CA
 revocation-check crl
 match certificate CRL-OVERRIDE override cdp url http://www.cisco.com/security/pki/crl/crca2048.crl
!
```

OCSP 확인

<#root>

```
! Sample A: OCSP from the certificate


crypto pki trustpiont ROOT-CA
 revocation-check ocsp
!

! Sample B: Override OCSP in certificate


crypto pki certificate map OCSP-OVERRIDE 1
 issuer-name eq root-ca.cisco.com
 subject-name eq root-ca.cisco.com
 alt-subject-name co cisco.com
!
crypto pki trustpoint ROOT-CA
 revocation-check ocsp
 match certificate OCSP-OVERRIDE override ocsp 1 url http://ocsp-responder.cisco.com
!
```

OCSP 및 CRL 검사 순서 지정

<#root>

```
! Check CRL if failure, check OCSP


crypto pki trustpoint ROOT-CA
 revocation-check crl ocsp
!
```

CN(Common Name) 및 SAN(Subject Alternate Name) 확인 사용

인증서의 CN 또는 SAN이 session target dns: 명령의 호스트 이름과 일치하는지 확인하도록 CUBE를 구성할 수 있습니다. IOS-XE 17.8+에서는 tls 프로파일을 통해 TLS 프로파일을 구성할 수 있습니다.

IOS-XE 17.8+

<#root>

```
Router(config)#
voice class tls-profile 1

Router(config-class)#
cn-san validate ?

  bidirectional Enable CN/SAN validation for both client and server certificate
  client Enable CN/SAN validation for client certificate
  server Enable CN/SAN validation for server certificate
```

클라이언트/서버 지정은 TLS 핸드셰이크의 피어 디바이스 역할을 참조한다는 점에 유의하십시오

자세한 설명을 보려면 다음을 수행합니다.

- cn-san validate server: CUBE는 아웃바운드 TLS 연결에 대해 수신된 피어 서버 인증서의 호스트 이름 검증을 수행합니다. 여기서 CUBE는 클라이언트 역할입니다.
- cn-san validate client: CUBE는 CUBE가 서버 역할인 인바운드 TLS 연결에 대해 수신된 피어 클라이언트 인증서의 호스트 이름 검증을 수행합니다.
- cn-san validate bidirection: TLS 핸드셰이크 중에 두 피어 역할에 대해 호스트 이름 검증을 활성화합니다.

cn-san validate client 명령(또는 양방향)을 사용할 경우 세션 대상이 확인됨은 아웃바운드 연결 및 cn-san validate server에 대해서만 적용되므로 SAN을 구성하여 확인해야 합니다.

클라이언트 호스트 이름 검증:

```
!
voice class tls-profile 1
 cn-san validate client
 cn-san 1 *.example.com
 cn-san 2 subdomain.example.com
!
```

서버 호스트 이름 검증:

```
!
```

```
voice class tls-profile 1
 cn-san validate server
!
sip-ua
 crypto signaling default tls-profile 1
!
dail-peer voice 1 voip
 session target dns:subdomain.example.com
!
```

17.8.1 이전

참고: 서버 호스트 이름 검증만 이 방법을 통해 사용할 수 있습니다.

<#root>

```
!
sip-ua
 crypto signaling default trustpoint TEST
```

cn-san-validate server

```
!
dail-peer voice 1 voip
 session target dns:subdomain.example.com
!
```

TLS 핸드셰이크 내에서 CUBE의 FQDN 호스트 이름을 사용하는 SNI(Server Name Indication) TLS 1.2 확장을 피어 디바이스로 전송하여 호스트 이름 유효성 검사를 원활하게 수행하도록 CUBE를 구성할 수도 있습니다.

```
!
voice class tls-profile 1
 sni send
!
sip-ua
 crypto signaling default tls-profile 1
!
```

CUBE의 Mutual TLS에 대한 참고:

- 기본적으로 CUBE가 TLS 서버(인바운드 TLS 연결 읽기) 역할을 하는 경우 항상 클라이언트 인증서를 요청합니다. 이 동작을 비활성화할 컨피그레이션이 없습니다.
- CUBE가 TLS 클라이언트 역할을 하고 아웃바운드 TLS 연결을 시작할 때 상호 TLS는 피어 디바이스가 TLS 서버 역할을 합니다. 이 시나리오에서 피어 디바이스는 CUBE에서 클라이언트 인증서를 요청하지 않을 수 있습니다.
- 이 두 시나리오 모두 CUBE가 전송하는 인증서 체인은 TLS 프로파일 또는 crypto signaling 명

령에 정의된 신뢰 지점에 의해 제어됩니다.

<#root>

```
!
sip-ua
 crypto signaling default
trustpoint CUBE-ENT


!
! OR
voice class tls-profile 1


trustpoint CUBE-ENT


!
sip-ua
 crypto signaling default tls-profile 1
!
```

원격 TLS 연결을 특정 신뢰 지점에 매핑

암호화 시그널링 기본 sip-ua 명령을 사용하는 경우 모든 인바운드 TLS 연결은 tls-profile 또는 개별 post-fix 명령을 통해 이러한 컨피그레이션에 매핑됩니다. 또한 인증서 검증을 수행할 때 사용 가능한 모든 신뢰 지점이 점검됩니다.

정의하는 보안 매개변수가 해당 TLS 세션에 정확하게 적용되도록 하려면 IP 주소를 기반으로 특정 피어 디바이스에 대해 특정 TLS 프로파일 컨피그레이션을 생성하는 것이 바람직할 수 있습니다. 이렇게 하려면 crypto signaling remote-addr 명령을 사용하여 tls-profile 또는 postfix 명령 집합에 매핑할 IPv4 또는 IPv6 서브넷을 정의합니다. 또한 client-vtp) 명령을 통해 직접 검증 신뢰 지점을 매핑하여 어떤 신뢰 지점이 피어 인증서의 검증에 사용되는지 정확하게 잠글 수 있습니다.

아래 명령은 지금까지 논의된 대부분의 항목을 요약합니다.

```
!
voice class tls-cipher 1
 cipher 1 ECDHE_RSA_AES128_GCM_SHA256
 cipher 2 ECDHE_RSA_AES256_GCM_SHA384
!
voice class tls-profile 1
 trustpoint CUBE-ENT
 cn-san validate bidirectional
 cn-san 1 *.example.com
 cipher 2
 client-vtp PEER-TRUSTPOINT
 sni send
!
sip-ua
 crypto signaling remote-addr 192.168.1.0 /24 tls-profile 1
```

```
!
```

이전 버전의 경우 다음과 같이 수행할 수 있습니다.

```
!
sip-ua
 crypto signaling remote-addr 192.168.1.0 /24 trustpoint CUBE-ENT cn-san-validate server client-vtp PEE
!
```

17.8부터는 음성 클래스 테넌트당 tls-profile 및 테넌트당 수신 대기 포트를 구성하여 지정된 수신 대기 포트에 추가 세그멘테이션 옵션을 제공할 수도 있습니다.

```
!
voice class tenant 1
 tls-profile 1
 listen-port secure 5062
!
```

엄격한 SRTP 적용

CUBE Enterprise에서 SRTP를 활성화할 경우 기본 작업은 RTP로의 대체를 허용하지 않는 것입니다.

가능한 경우 모든 통화 레그에서 SRTP를 사용하지만 기본적으로 CUBE는 필요에 따라 RTP-SRTP를 수행합니다.

CUBE는 16.11+에서 시작하는 디버깅에서 SRTP 키를 로깅하지 않습니다

```
!
voice service voip
 srtp
!
! or
!
dial-peer voice 1 voip
 srtp
!
```

안전하지 않은 SRTP 암호 자르기

기본적으로 모든 SRTP 암호는 제안을 생성할 때 CUBE에서 전송합니다. 관리자는 IOS-XE

16.5+에서 voice class srtp-crypto 명령을 사용하여 차세대 AEAD 암호 모음과 같이 더 안전한 암호로 축소할 수 있습니다.

또한 이 컨피그레이션은 CUBE가 SRTP 암호를 선택하고 사용 가능한 여러 옵션이 있는 일부 제안에 대한 응답을 생성할 때 사용되는 기본 환경 설정을 변경할 수 있습니다.

참고: 일부 오래된 Cisco 디바이스 또는 피어 디바이스는 AEAD 암호를 지원하지 않을 수 있습니다. 암호 그룹을 트리밍할 때 해당되는 모든 문서를 참조하십시오.

<#root>

```
Router(config)#
voice class srtp-crypto 1

Router(config-class)#
crypto ?
  <1-4> Set the preference order for the cipher-suite (1 = Highest)

Router(config-class)#
crypto 1 ?

  AEAD_AES_128_GCM        Allow secure calls with SRTP AEAD_AES_128_GCM cipher-suite
  AEAD_AES_256_GCM        Allow secure calls with SRTP AEAD_AES_256_GCM cipher-suite
  AES_CM_128_HMAC_SHA1_32 Allow secure calls with SRTP AES_CM_128_HMAC_SHA1_32 cipher-suite
  AES_CM_128_HMAC_SHA1_80 Allow secure calls with SRTP AES_CM_128_HMAC_SHA1_80 cipher-suite
```

```
!
voice class srtp-crypto 1
 crypto 1 AEAD_AES_256_GCM
 crypto 2 AEAD_AES_128_GCM
!
voice service voip
 sip
  srtp-crypto 1
!
! or
!
voice class tenant 1
 srtp-crypto 1
!
! or
!
dial-peer voice 1 voip
 voice-class srtp-crypto 1
!
```

기타 사용하지 않는 VoIP 프로토콜 비활성화

이 게이트웨이에서 H323, MGCP, SCCP, STCAPP, CME, SRST를 사용하지 않는 경우 CUBE를 강화하기 위해 컨피그레이션을 제거할 필요가 있습니다.

H323을 비활성화하고 SIP 간 통화만 허용

```
!
voice service voip
 allow-connections sip to sip
 h323
  call service stop
!
```

MGCP, SCCP, STCAPP, SIP 및 SCCP SRST를 비활성화합니다.

참고: 이러한 명령 중 일부는 다른 모든 컨피그레이션을 삭제하고, 완전히 제거하기 전에 기능이 사용되지 않는지 확인합니다.

<#root>

```
Router(config)#
no mgcp

Router(config)#
no sccp

Router(config)#
no stcapp

Router(config)#
no voice register global

Router(config)#
no telephony-service

Router(config)#
no call-manager-fallback
```

통화 라우팅 및 요금 사기

신뢰할 수 있는 IP로부터의 연결 허용

기본적으로 CUBE는 다이얼 피어 세션 대상 및 음성 클래스 서버 그룹 컨피그레이션에 구성된 IPv4 및 IPv6 주소로부터의 인바운드 연결을 신뢰합니다.

추가 IP 주소를 추가하려면 음성 서비스 voip를 통해 구성된 ip address trusted list 명령을 사용합니다.

앞서 설명한 CN/SAN 검증 기능을 통해 클라이언트/서버 호스트 이름 검증이 SIP TLS와 함께 구성된 경우, CN/SAN 검증이 성공하면 IP 주소의 신뢰할 수 있는 목록 확인이 무시됩니다.

CUBE에서 모든 인바운드 연결을 허용하도록 신뢰할 수 있는 ip 주소를 사용하지 마십시오.

```
!
voice service voip
 ip address trusted authenticate

 ip address trusted list
  ipv4 192.168.1.1
  ipv4 172.16.1.0 /24
!
```

show ip address trusted list를 사용하여 IP 주소 확인 및 다른 컨피그레이션에서 파생된 모든 정적 및 동적 신뢰 목록 정의의 상태를 볼 수 있습니다.

다이얼 피어가 종료되거나 킵얼라이브 검사에 실패한 후 다운 상태로 설정되면 다이얼 피어/서버 그룹에서 파생된 동적 값이 신뢰할 수 있는 목록에서 제거됩니다.

기본적으로 인바운드 통화가 IP Trusted(IP 신뢰) 목록을 통과하지 못할 경우 자동으로 삭제되지만 no silent-discard untrusted voice service(no silent-discard 신뢰할 수 없는 음성 서비스) voip > sip 명령을 사용하여 발신자에게 오류를 다시 보낼 때 이를 재정의할 수 있습니다. 그러나 공격자는 이 응답을 사용하여 디바이스가 실제로 SIP 트래픽을 수신 대기하고 있음을 나타내고 공격 작업을 가속화할 수 있습니다. 이러한 자동 삭제는 IP Trusted List 삭제를 처리하는 기본 방법입니다.

일반 다이얼 피어 라우팅 방지

destination-pattern과 같은 일반적인 "모두 탐지"대상 패턴을 사용하면 CUBE를 통해 사기성 통화를 라우팅할 가능성이 높아질 수 있습니다.

관리자는 알려진 전화 번호 범위 또는 SIP URI에 대한 통화만 라우팅하도록 CUBE를 구성해야 합니다.

CUBE 통화 라우팅 기능에 대한 자세한 설명은 다음 문서를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html

CUBE 위협 완화

잘못된 형식의 패킷 처리

기본적으로 CUBE는 SIP 및 RTP 패킷을 검사하여 오류를 확인하고 패킷을 삭제합니다.

비인가 RTP 패킷

기본적으로 IOS-XE CUBE는 SIP SDP 제안/응답 신호 처리를 통해 협상된 연결만 허용하여 모든 RTP/RTCP 스트림에 대해 소스 포트 검증을 수행하며 비활성화할 수 없습니다.

다음 명령을 확인하여 모니터링할 수 있습니다.

```
show platform hardware qfp active feature sbc global | s Total packets dropped|Dropped packets:
```

CUCM과의 interop의 경우 포트 4000에서 제공되는 대기 중 음악이 삭제되지 않도록 Cisco CallManager Service를 통해 듀플렉스 미디어 스트리밍을 활성화하는 것이 좋습니다.

RTP 포트 범위 강화

기본적으로 IOS-XE는 8000~48198의 포트 범위를 사용합니다. 이 명령은 다음 명령을 통해 16384~32768과 같은 다른 범위로 구성할 수 있습니다.

```
!
voice service voip
 rtp-port range 16384 32768
!
```

관리자는 IPv4 및 IPv6 주소 범위별로 RTP 포트 범위를 구성할 수도 있습니다.

이 컨피그레이션을 사용하면 IP 및 포트 범위가 정적으로 정의되므로 CUBE의 VoIP 애플리케이션에서 이러한 패킷을 라우터의 CPU에서 UDP 프로세스로 입력하지 않음으로써 팬텀 패킷 처리를 보다 효율적으로 수행할 수 있습니다. 이렇게 하면 CPU 펀팅 동작을 우회하여 많은 수의 합법적 또는 부적격 RTP 패킷을 처리할 때 높은 CPU를 완화하는 데 도움이 됩니다.

```
voice service voip
 media-address range 192.168.1.1 192.168.1.1
  port-range 16384 32768
 media-address range 172.16.1.1 172.16.1.1
  port-range 8000 48198
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_phantom-packet-handling.html

DOS(Denial of Service) 방지

총 통화, CPU, 메모리, 대역폭을 기준으로 통화를 제한하도록 통화 허용 제어 기능을 활성화할 수 있습니다. 또한 통화 스파이크를 탐지하여 통화를 거부하고 서비스 거부를 방지할 수 있습니다.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-cube-call-admission-control.html

주소 숨기기

기본적으로 CUBE는 SIP 헤더의 IP 주소(예: Via, Contact 및 From)를 자체 IP 주소로 대체합니다.

음성 서비스 voip 명령 주소 숨기기를 적용하여 Refer-To, Referred-By, 3xx 연결 헤더, History-Info, Diversion 헤더로 확장할 수 있습니다.

또한 이 헤더 값에 포함될 수 있는 각 통화 레그 완화 IP 주소에 대해 새 통화 ID가 생성됩니다.

주소를 숨기기 위해 IP 주소 대신 호스트 이름이 필요한 경우 voice-class sip localhost dns:cube.cisco.com 명령을 구성할 수 있습니다.

발신자 ID 프라이버시

CUBE는 임의의 다이얼 피어에 구성된 명령 clid-strip name과 함께 SIP 헤더에서 발신자 ID 이름 값을 삭제하도록 구성할 수 있습니다.

또한 CUBE는 PPID(P-Preferred Identity), PAID(P-Asserted Identity), 프라이버시, PCPID(P-Called Party Identity), RPID(Remote-Party Identity)와 같은 SIP 프라이버시 헤더를 연동하고 이해할 수 있습니다. 자세한 내용은 다음 문서를 참조하십시오. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-paid-ppid-priv.html

SIP 다이제스트 인증

CUBE가 서비스 공급자에 SIP 등록하는 동안 또는 통화 시그널링 업스트림 UAS 장치가 401 또는 407 상태 코드를 CUBE의 인증에 도전하는 적용 가능한 WWW-Authenticate/Proxy-Authenticate 헤더 필드와 함께 반환할 수 있습니다. 이 핸드셰이크 중에 CUBE는 후속 요청에서 Authorization 헤더 필드 값을 계산하기 위한 MD5 알고리즘을 지원합니다.

지원되지 않는 SIP 헤더 또는 SDP

CUBE는 지원되지 않는 SIP 헤더 또는 SDP가 인식되지 않는 것을 제거합니다. pass-thru content sdp, pass-thru content unsupp 또는 pass-thru header unsupp와 같은 명령을 사용할 경우 어떤 데이터가 CUBE를 통과하는지 확인해야 합니다.

SIP 헤더 또는 SDP 제거 또는 수정

추가 제어가 필요한 경우 관리자가 SIP 헤더 또는 SDP 특성을 유연하게 수정하거나 완전히 삭제하도록 인바운드 또는 아웃바운드 SIP 프로필을 구성할 수 있습니다.

SIP 프로필 사용에 대한 다음 문서를 참조하십시오.

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi-sip-param-mod.html
- https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html#anc45

기타 보안 기능

암호화된 비밀번호

CUBE에서는 실행 중인 컨피그레이션에서 SIP 등록 및 기타 IOS-XE 비밀번호를 암호화하려면 16.11 이상 버전의 암호화된 비밀번호가 필요합니다.

```
password encryption aes
key config-key password-encrypt cisco123
```

액세스 목록

신뢰할 수 있는 목록 기능은 CUBE 애플리케이션 내의 레이어 7에서 작동합니다. 패킷이 자동으로 삭제될 때까지 CUBE는 이미 패킷 처리를 시작했습니다.

인바운드 또는 아웃바운드 레이어 3 또는 4 액세스 목록의 인터페이스를 잠가 라우터의 진입점에서 패킷을 삭제하는 것이 바람직할 수 있습니다.

이렇게 하면 CUBE의 CPU 주기가 합법적인 트래픽에 사용됩니다. IP Trusted List(IP 신뢰 목록) 및 Hostname Validation(호스트 이름 검증)과 함께 ACL은 CUBE 보안에 대한 계층화된 접근 방식을 제공합니다.

영역 기반 방화벽(ZBFW)

Cisco CUBE는 IOS-XE ZBFW와 함께 구성하여 애플리케이션 검사 및 기타 보안 기능을 제공할 수 있습니다.

이 항목에 대한 자세한 내용은 CUBE 및 ZBFW 가이드를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-border-element/220378-configure-zone-based-firewall-zbfw-co.html

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.